REMARKS

Background

The present disclosure relates to the provision by a location server of location data that represents the location of a mobile entity. Claim 1 as originally worded simply refers to "location data about a mobile entity" which has been taken by the Examiner to include location data about base stations in a mobile network (this data being required to enable the mobile entity to determine its own location).

According to amended claim 1 the location server provides the location data in encrypted form to a recipient that is either the mobile entity or a service system for "providing a location-based service to the mobile entity using the location data as an input'. The recipient does not itself decrypt the location data itself but rather uses the services of a "decryption entity" to recover the unencrypted location data.

One reason for this arrangement, as opposed to providing the location data in an encrypted form that the recipient can decrypt, is that billing for location data can now be carried out when the location data is decrypted (generally immediately prior to use). This means that a billing model can be implemented in which, in effect, only usage of location data is charged for and not its mere provision. This billing feature was the subject of original claims 19 and 20, but claim 1 has now been amended to include this feature. At the same time claim 1 has been rewritten to clarify the operations involved.

In addition to deleting claims 19 and 20 (due to the inclusion of their subject matter in amended claim 1) claims 21 and 22 have been cancelled as the subject matter of these claims is adequately covered in other applications.

Claim 23 has also been deleted and the independent apparatus claim 24 amended into line with the amendments made to claim 1.

A new independent method claim 31 that is a near equivalent of original claims 1, 2 and 5, and a dependent claim 32 that corresponds to original claim 6, have been

added. These claims are not limited to the billing feature added to independent claims 1 and 24.

US 6,671,377 – Havinis

The main reference relied upon by the Examiner is Havinis; the Examiner alleges that this reference anticipates original claim 1 and, also, the combination of this claim with original claim 19 (the original billing feature claim).

Havinis teaches sending encrypted "network information" to a mobile stations (MS) where "network information" is information such as BTS coordinates (col. 3, lines 2-3). This network information is required by the MS to enable it to calculate its location. The intention appears to be to keep the network information confidential; previous teaching was to include this type of information in clear in signaling channels.

The network information is encrypted using a key K_L based on:

-the subscriber identification key known to both the network Home Location Register (HLR) and the MS (see col.5 lines 50-56 and col.5, line 67 to col.6, line 2);

-a positioning indication 218 provided by the MS that "indicates to the network 10 the number and/or duration of the positionings that the MS 20 will be performing" (see col.5, lines 41-44);

-a random number (RAND) generated in the network by the Authentication Center (see col.5, lines 50-53).

The generation of the key K_L is described at col.5 lines 45-62. The key K_L is then used by the BSC to encrypt the network information which is then sent to the MS. The random number RAND is broadcast unencrypted by the MSC (see col.6, lines 7-11).

The MS itself generates the key K_L using the subscriber identification key and positioning indication already in its possession, and the broadcast random number RAND. Having generated the key K_L the MS uses it to decrypt the received encrypted network information (see col.6, lines 12-27). The network information is then used in

the determination of the location of the MS (see col.6, lines 28-42). Finally, the location of the MS is sent to a location application LA 280 (see col.6, lines 54-62). The location application is apparently deemed by the Examiner to corresponds to the service system of the present claims. It may be noted that no special measures appear to be taken in Havinis to protect the location data representing the location of the MS.

The following differences exist between Havinis and the amended Claim 1:

-Havinis is concerned with encrypting "network information" passed from the network to the MS whereas amended Claim 1 concerns encrypted "location data that represents the location of the mobile entity" that is passed from a location server to a recipient;

-the encrypted network information is decrypted by the MS in Havinis whereas in amended Claim 1 the recipient cannot decrypt the encrypted location data but must use "a decryption entity that is not under the control of the recipient" to carry out decryption;

-in Havinis, billing clearly takes place on the basis of the network information provided rather than on the basis of the decryption of location data as in amended Claim 1.

With respect to this last distinction, whilst in Havinis the provision of network information directly leads to its decryption, this does not remove the distinction being made – deferring billing until decryption has occurred has the advantage already stated, namely that it is possible to defer billing until the location data is actually put to use.

More important to note is that the Examiner has apparently misinterpreted the passage at col.3, lines 46-49 of Havinis. The Examiner believes that this passage discloses the billing feature of original claim 19 (see item 10 in the official action). The passage reads:

"Advantageously, the encryption and deciphering process of the present invention can be utilized by the network to charge a mobile subscriber either on a per positioning request basis or on a positioning duration basis."

The examiner incorrectly reads this as meaning that charging is effected when decryption is carried out. So far as Havinis is concerned, the encryption and deciphering process is a single process and there is no explicit teaching as to when billing is triggered. In fact, the only reference to charging or billing a subscriber in the whole of Havinis is the quoted passage. It is, however, possible to deduce how charging is effected by careful study of the words used in the passage. Thus, it is first to be noted that the passage is talking about charging by the network – this means that the network must be provided with the relevant data. Next, it is to be noted that the subscriber is to be charged "either on a per positioning request basis or on a positioning duration basis". It is these very factors that are detailed in the "positioning indication 218" that is passed from the MS to the MSC 14 (col.5, lines 41-44). It therefore reasonable to assume that the network carries out charging on the basis of the positioning indicator passed to it (subject to satisfactory provision of the network information requested). In other words, charging is based on provision of the network information according to the details of the request from the MS. Any other interpretation of the quoted passage would appear to be mere speculation driven by an ex post facto analysis of Applicants' claims.

US 6,377,688 – Numao

The Examiner rejected additional claims on the basis of Havinis in view of Numao (see paragraph 23 of the official action). Numao discloses a cryptographic arrangement in which a decryption server 130 generates public and private keys and publishes the public key (col 3, lines 57-61). A message sender 110 uses the public key to encrypt a message for sending to a receiver 120; the receiver on receiving the encrypted message, blinds it using a random secret number and sends the blinded, encrypted message to the decryption server that decrypts the message and returns the still blinded, but now decrypted message, to the receiver. Finally, the receiver uses the random secret to unblind the message and recover it in plaintext (see col. 1, line 61 through col.2, line 6).

The terms "blinding" and "unblinding" are the terms frequently used for this type of operation by persons skilled in the art (as is suggested at col.3, line 65 of Numao).

One advantage of this arrangement is said to be that neither the sender nor receiver has to manage the storage of a secret – in fact, this is only partly true as the receiver must store his random secret number at least for a short time.

However, the main advantage asserted for Numao appears to be that decryption server can provide assurance to the sender that only a trusted receiver will be served by the decryption server (col.2, lines 58-61).

So far as can be seen, there is no motivation for a person skilled in the art to combine Havinis and Numao. The type of mobile station MS used by Havinis is well equipped for storing and managing a secret, this being part of its normal operation so there is no particular advantage to be gained by incorporating the teaching of Numao in this respect into Havinis; in fact, it is believed that there are very definite drawbacks arising from the extra complexity involved (the provision of a decryption server and the requirement for extra processing and messaging) since at the very least, the suggested combination is more complex and thus more costly. People skilled in the art do not make systems more complex and/or more costly without obtaining some advantage in exchange. The advantage of Numao of providing assurance to the sender that only a trusted receiver will receive the decrypted message, is redundant in Havinis as the mobile network is already best placed to ensure that the correct MS receives the network information – providing a decryption server for this purpose is appears to be rather pointless.

It is submitted that the Examiner is using Applicants' claims as a road map to the prior art as opposed to considering what the prior art actually teaches. The combination asserted by the Examiner is based on hi9ndsight reconstruction.

Moreover, even if it were obvious to combine Havinis and Numao, the resulting combination would not teach the invention as set out in claim 1 since the combination would still only be concerned with network information (and not mobile entity location) and would not generate a billing record at the point of decryption.

The Dependent Claims

While it is not necessary to discuss all of the rejections of the dependent claims, the applicant would like to address the rejection of claims 5 and 6.

Claim 5 concerns an embodiment where the location data is provided by the location server to the mobile entity which then passes it on to the service system, this latter arranging for the decryption entity to decrypt and return the location data. This is the preferred embodiment. In terms of Havinis, it would require encrypted location data to be passed to the location application LA and for the latter to then contact a decryption entity to have it decrypted. Clearly, there is nothing like this in Havinis. Furthermore, as Havinis does not describe the encrypting of the MS location data passed to the LA, there would appear to be no reason to introduce the teaching of Numao.

Claim 6 concerns two authentication checks carried out by the decryption entity. Claim 6 recites that "the service system" passes "the identity data to the decryption entity which authenticates the identity data and only returns the decrypted location data to the service system if both:

- the mobile entity indicated by the identity data is the same as the one to which the location data relates, and
- service system indicated by the identity data is the same as the one asking the decryption entity to decrypt the location data."

The Examiner is correct in noting that Numao does disclose that the decryption server checks that the receiver is the same as indicated in a certificate sent by the sender – see the example given between lines 19 and 42, at column 6. The Examiner attempts to read this on claim 6. However, since claim 6 recites that two checks are required (which are quoted above), it is not understood how the Numao patent, which apparently only teaches carrying out one check and not the two different checks as required by claim 6, can be used to assert that claim 6 is not patentable.

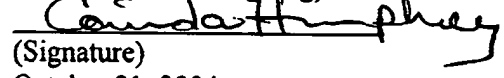
The Other Independent Claims

The independent apparatus claim 24 was been amended in a similar vein as Claim 1 and thereof it is believed to be patentable over the cited art. .

The new independent claim 31 is distinguished from the references cited for the same reasons as already given in respect of claim 5. Similarly, dependent claim 32 is further distinguished by the same reasons as given in respect of claim 6.

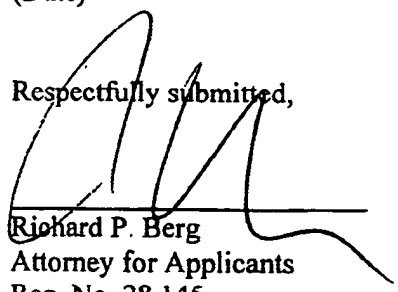
The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on
October 21, 2004
(Date of Deposit)
Corinda Humphrey
(Name of Person Signing)



(Signature)
October 21, 2004
(Date)

Respectfully submitted,



Richard P. Berg
Attorney for Applicants
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300